

אלגוריתם אוקלידי

-/c N

$$f(x) = x^5 + x^3 + x^2 + x + 1$$

$$g(x) = x^4 + x^3 + x$$

$$\gcd(f, g) \sim /c \mathbb{Z}_N$$

$$\begin{array}{r} x-1 \\ x^5 + x^3 + x^2 + x + 1 \end{array} \Bigg| x^4 + x^3 + x \Rightarrow f(x) = (x-1)g(x) + 2x^3 + 2x + 1$$

$$\begin{array}{r} -x^5 + x^4 + x^2 \\ \hline -x^4 + x^3 + 0 \\ -x^4 + x^3 - x \\ \hline 2x^3 + 2x + 1 \end{array}$$

מחלקים כזה, רשיון -

$$\gcd(f, g) = \gcd(g, r_1)$$

(קטנוצוג מחלקים המשותפים של f ו- g שווה לקטנוצוג מחלקים

המשותפים של g ו- r_1 .)

$$\begin{array}{r} -x-1 \\ x^4 + x^3 + x \end{array} \Bigg| 2x^3 + 2x + 1 \rightarrow r_2 = 2x^2 + x + 1$$

$$g = \underbrace{(-x-1)}_{q_2} \underbrace{(2x^3 + 2x + 1)}_{r_1} + \underbrace{2x^2 + x + 1}_{r_2}$$

נחלק r_2 ב- r_1 כדי לקבל $r_3 = 0$

$$\begin{array}{r} x+1 \\ 2x^3 + 2x + 1 \end{array} \Bigg| 2x^2 + x + 1 \rightarrow r_3 = 0$$

$$\underbrace{(2x^3 + 2x + 1)}_{r_1} = \underbrace{(x+1)}_{q_3} \underbrace{(2x^2 + x + 1)}_{r_2}$$

$$\gcd(r_1, r_2) = r_2, \text{ מכיוון } r_2 | r_1$$

($1 = 1/8 \text{ PZPN}$) $\gcd$ ב- $\mathbb{Z}_N$

$$N \nmid N \text{ ב-} r_2 \leftarrow r_2 = 2x^2 + x + 1$$

$$N \nmid N \text{ ב-} \frac{1}{2} r_2$$

$$\frac{1}{2} r_2 = -1 \cdot r_2 = -2x^2 - x - 1 = x^2 + 2x + 2$$

הזכרנו שיש לנו פולינומים f, g , יש הרבה דרכים

$$\gcd(f, g) = a \cdot f + b \cdot g \quad \text{כאשר } a(x), b(x) \text{ פולינומים}$$

אלגוריתם אוקלידי מזהיר אותנו שמצאנו a, b כאלה. למשל

$$\gcd(f, g) = -r_2 = -(g - q_2 r_1) \quad \text{שכן:}$$

$$\begin{aligned} \ominus - (g - r_2(f - r_1 g)) &= -g + r_2(f - r_1 g) = \\ &= -g + r_2 f - r_1 r_2 g = r_2 f + (r_1 r_2 - 1)g = \\ &= (-x-1)f - (2-x^2)g \end{aligned}$$

$$\begin{aligned} f &= q_1 g + r_1 \\ g &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \end{aligned}$$

מסקרה חלופה מאלגוריתם אוקלידס:

* אם f, g פולינומים "זרים", כלומר

$$\gcd(f, g) = 1$$

$$af + bg = 1 \quad \text{עם } a, b$$

$$\begin{aligned} 1 + q_1 q_2 &= \\ &= 1 + (-x-1)(x-1) = \\ &= 1 + (1-x^2) = 2-x^2 \end{aligned}$$

פריקת זא-פריקת של פולינומים:

יהי f פולינום בדרגה לא קטנה מ-1, כלומר, $\deg f \geq 1$,

אז f נקרא פריק, אם ניתן לכתוב אותו כמכפלה של פולינומים

ממעלה חיובית ($\deg > 0$). $f = g \cdot h \leftarrow \deg g, \deg h \geq 1$

אחרת f נקרא אי-פריק.

משפט - יהי $f \in F[x]$ ואז ניתן לכתוב אותו כמכפלה

של פולינומים אי-פריקים. נחמה על זה/יחידה לצד כדי סדר הפירוקים, וסדר איברים הפירוקים.

דוגמה - כל פולינום ממעלה 1 הינו אי-פריק

הוכחה - יהי f פולינום ממעלה 1. אנו רוצים לראות $f = g \cdot h$

$$1 = \deg f = \deg g + \deg h$$

מסמלים שלמים ואי-שלמים.

$$\Leftarrow \text{אם } \deg g = 0 \text{ או } \deg h = 0$$

משפט - יהי $P \neq 0 \in F[x]$, ויהי $\alpha \in F$, אז α שורש של P

$$x - \alpha \mid P \quad \text{אם } \alpha \text{ שורש של } P$$